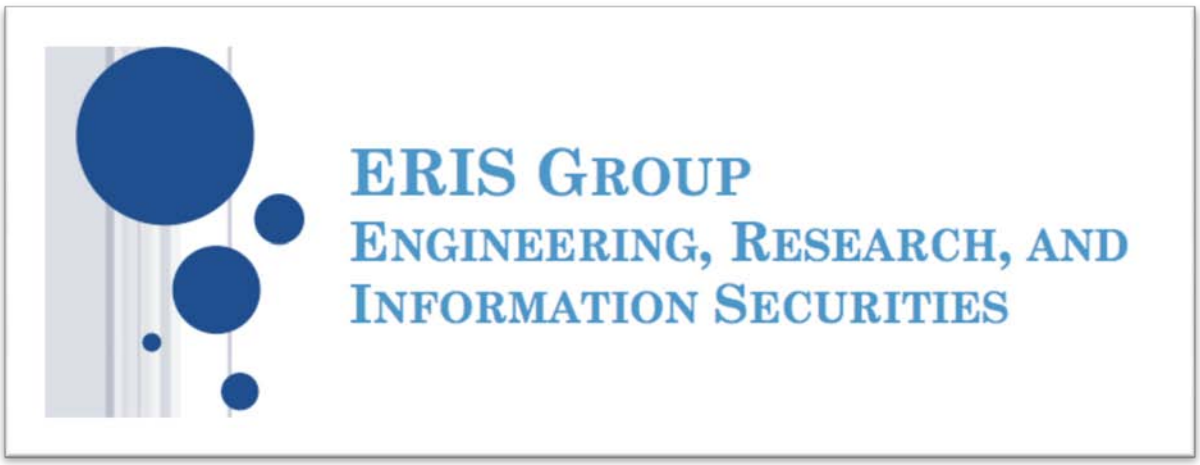


CORPORATE THREAT MODEL

May 1st 2009

Authors:
Shaun Deaton (srdeaton@indiana.edu)
Emily K. Adams (ekadams@indiana.edu)
Mehool Intwala (mintwala@indiana.edu)
Tak Lon Wu (taklwu@indiana.edu)

Table of Contents

1 Use Scenarios 3
2 External Dependencies 5
3 Implementation Assumptions 7
4 External Security Notes 8
5 Internal Security Notes 10
6 Trust Levels 11
7 Entry Points 12
8 Assets 13
9 Data Flow Diagrams 15
10 Threats 17
11 Vulnerabilities 23
12 Threat Tree Diagrams ..... **Error! Bookmark not defined.**

INTRODUCTION

The ERIS Group – Engineering, Research, and Information Securities – is a small engineering firm that specializes in designing [redacted] (classified) for the Department of Defense Advanced Weapons Division. Our company comprises of an engineering department and a finance department. Our employee base consists of two department managers (engadmin, finadmin), four security engineers (graduate), five departmental staff (staff1 – staff4), and one mailroom employee (staff5).

The ERIS Group approaches system and data protection very seriously. With high-profile clients like the Department of Defense we control data access and protect network traffic by restricting our services to only those necessary for ERIS to provide advanced products. Our technology architecture, services, and server configurations maintain this standard of high-level data protection our customers expect.

1 Use Scenarios

Listed below are the expected uses of the Eris information technology infrastructure. Not deploying the architecture with these specifications will impact the security of network and greatly increase the potential for compromised data.

ID	Description
1	Expected to have reliable power and data lines entering company's infrastructure.
2	Expect secure data channels dedicated to only to Department of Defense.
3	Firewalls are intended to keep the good traffic in and let the malicious traffic out.
4	The implementation and configuration of our private corporate network is intended to serve only our employees.
5	Intend for users' to have strong passwords and to input them by hand every time, and not have application remember it.
6	It is assumed that the company's physical facilities will be safe from harm and protected from those with malicious intent

2 External Dependencies

The external dependencies below are assumptions made about the usage or behavior of the Eris' IT infrastructure and the consequences of failure to follow these assumptions.

ID	Description
1	Connected to public electric grid, with no backup generator or other power source. So, subject to the whims of power outages.
2	Servers require certain environments for dependable operation; temperature and humidity must be controlled. Power and/or mechanical failures in environmental controls can cause damage and other malfunction in hardware.
3.0	Most all hardware and software are commercial; and there is not much customization past the configuration options. So, there may be some process or software module enabled by default that represents a potential vulnerability.
3.1	Depend upon downloaded server clients and other system infrastructure software to be the software it is supposed to be; i.e. check md5 hashes of source codes. Otherwise may contain malicious code or unintentional errors that hopefully the original hashed code did not have. Resulting in system crashes or takeover. (Note: Just having bugs in general should always be an assumption, whether they are purely security related or not.)
4	Communication bandwidth and integrity (requested or available, considering these relate to the external Internet Service Provider and internal networks respectively). Drops in expected bandwidth affects internal and external network efficiency; especially important when handling large volumes of data. Additionally, lost or damaged data

	may also be a possibility.
5	Company's clients' machines are expected to be secure and up to date; in order to avoid compromising company machines.

3 Implementation Assumptions

Implementation assumption guidelines related to system development that must be verified after system is running. (If X is implemented then it should not introduce security breaches.)

ID	Description
1	All software in use is consistently patched and upgraded when appropriate.
2	System is actually a small virtual subnet of a subnet with its own gateway; in totality, the entire system comprises four Linux boxes and one class-provided gateway managing the subnet. The main unit and a number of other boxes are grouped into their own subnets with nearly identical structure and functionality as ours. Must have all subgroups isolated on local network, so the main gateway is critical for security and overall functioning. Failure to use restricted IP ranges, for example, may result in security breaches.
3	Implement custom scripts for system monitoring, such as using NMAP and other techniques. Unexpected complications could arise, affecting performance and security. For example, an intense NMAP port scan may disrupt http traffic. Therefore, scripts must be tested for security conflicts in addition to performing their intended function; to automate some proactive security functions.
4	Implement automatic security updates using a scheduled apt-get. The concern with implementing apt-get automatically is that malformed or poorly programmed updates damage system causing failure or introducing new vulnerabilities.

4 External Security Notes:

Provide for secure system integration, non-default configuration details. Include guarantees and misuses. Often info found in user manual.(firewall, server configurations, Uptime, privacy)

ID	Description
1	Set password to minimum of 12 char with 3 character types. Have over 71^{12} possibilities. Consequences of not using complex enough password is a decrease in system security.
2	Have admin enforce strong passwords and password protection; even allow admin to monitor user passwords. Admin can access restricted data, making them a potential liability.
3	Secure servers and server location to prevent physical tampering. Damaging system, stealing hard drives, etc, may occur. (secure super computer as well)
4	System's local gateway secured behind custom firewall that is configured properly, to protect web, mail, and file servers behind their own custom firewalls. If these are not implemented or incorrectly implemented, then anyone can connect to system or could be keeping good users out.
5	Apache2 client installed in web server as an anonymous user restricted to access above its directory location. If apche2 is compromised it cannot be used to reach above its own local root. But, unknown if it may be able to compromise a jailed subdirectory.
6	Two jailed subdirectories created below Apache2 root directory used for hosting separate WebPages. This guarantees processes cannot enter or leave jail, so adversaries cannot hitch a ride out and gain that processes privileges.(did not implement)
7	https is enabled by default, important for secure online transactions. Otherwise traffic could be monitored for sensitive data.

8	All servers have a unique administrative password, increasing system wide security, as opposed to hack one, hack all.
9	Do not allow Web-based management of system, requires use of designated physical devices, such as terminal servers. Otherwise adversaries could gain web-based admin access.
10	Employees have private key given by admin to make a VPN connection from the internet. If keys are leaked then adversary can enter the VPN, posing as an employee.
11	Disable DHCP services and only admin assigns IP addresses to machines on the internal network. Failure will allow anyone to connect to the internal network.
12	Access Control Lists so only users who own the files have access to it. If this fails then users would gain a privilege elevation.
13	ssh port changed from the standard port of 22 to 2222
14	Admin name is Graduate – security thorough obscurity

5 Internal Security Notes:

Internal doc of threat model, security tradeoffs made for cost, etc. Assignment of liability, not security related not included.

ID	Description
1	Had only one router therefore restricted network topology. More routers would allow for DMZ setup.
2	Had only one network card per machine. This affects the ability to implement a DMZ and also did allow for the proper implementation of the VPN service.
3	Due to complications with jailing in the source code installation, it was not implemented due to time constraints.
4	Did not do TCP wrappers in this implementation, because it was determined that IPTables provided sufficient network traffic security.
5	High level physical system security, such as double key access, was not employed due to cost. Building security and card key access helps to mitigate this concern.

6 Trust Levels

ID	Name	Description
1	Administrator (Remote/Local)	The administrator can manage specific system functions for access and security
2	Employee	Company employees need a user account to access and use the system for job related duties
3	Client/guest	It is important for the company's clients & other guests to have accounts with certain privileges differing from employees, and each other.
4	System processes & software	Software & such runs at certain privilege levels.
5	External anonymous user	Anonymous user which connects from internet to the company's public webpage or attempts to connect to VPN server.

7 Entry Points

The following table lists the entry points and describes the interfaces through which external entities can interact with our systems. These entry points can either be a physical or virtual access points.

ID	Name	Description	Trust Level
0	Connection	The connection that users can physically or virtually connect to system.	(1) Administrator (2) Employee (3) Client/Guest (4) System processes & software (5) External anonymous user
1	VPN Connection	The external connect which allow employee to get an internal IP	(1) Administrator (2) Employee (5) External anonymous user
2	Open Service Ports (Incoming)	Service ports that listen to for network traffic	(1) Administrator (2) Employee (3) Client/Guest (4) System processes & software (5) External anonymous user
3	Physical Access to system	Physical access to system, i.e. can directly interact with hardware and special admin interfaces	(1) Administrator (2) Employee (Some)

8 Assets

The following table lists the assets and describes the resources or information that our system to need protected. Also, it shows the related Trust level to each item that can be accessed.

Note: Some aspects may be fictionalized, e.g. assuming a company that does medium to high-level contract work there should be an appropriate level of computational and memory resources; essentially assuming monetary expenditures in the hundreds-of-thousands at a maximum. This comes with the caveat that all such resources are still supported and secured by the four server infrastructure already introduced.

ID	Name	Description	Trust Level
0	Access	Assets relate to the connection with the system, especially the VPN, file share, and internal web containing client info, project data, and hardware resources	(1) Administrator (2) Employee (3) Client / Guest
1	Hardware	Accounts for physical infrastructure of companies computer network and that of ISP	
1.1	Custom admin/employee stations	Each employee has their own custom station design specifically for the job function: as a company perk we allow and encourage suggestions & personalization; while of course	Entire Company

		adhering to proper security practices	
1.2	TerraFLOP supercomputer	An advanced terra flop super computer on which engineers can request processing time	(1) Administrator (2) Employee
2	Users' account data	The data which is owned by users, such user accounts and passwords. (Including Manager level)	(1) Administrator (2) Employee (3) System processes & software
2.1	Users' personal data	My allow infiltration or theft of company/employee resources, such as social engineering attacks	(1) Administrator (2) Employee
3	Project Data	Data which is owned by Department level. And tied to company clients.	(1) Administrator (2) Employee (3) Clients
4	Public/Private website	The internal information (IPs, Ports) might be embedded within the web page, if the web page is not secure	(1) Administrator (2)Employee (3)Client/Guest (4) System processes & software (5) External anonymous user

9 Data Flow Diagrams

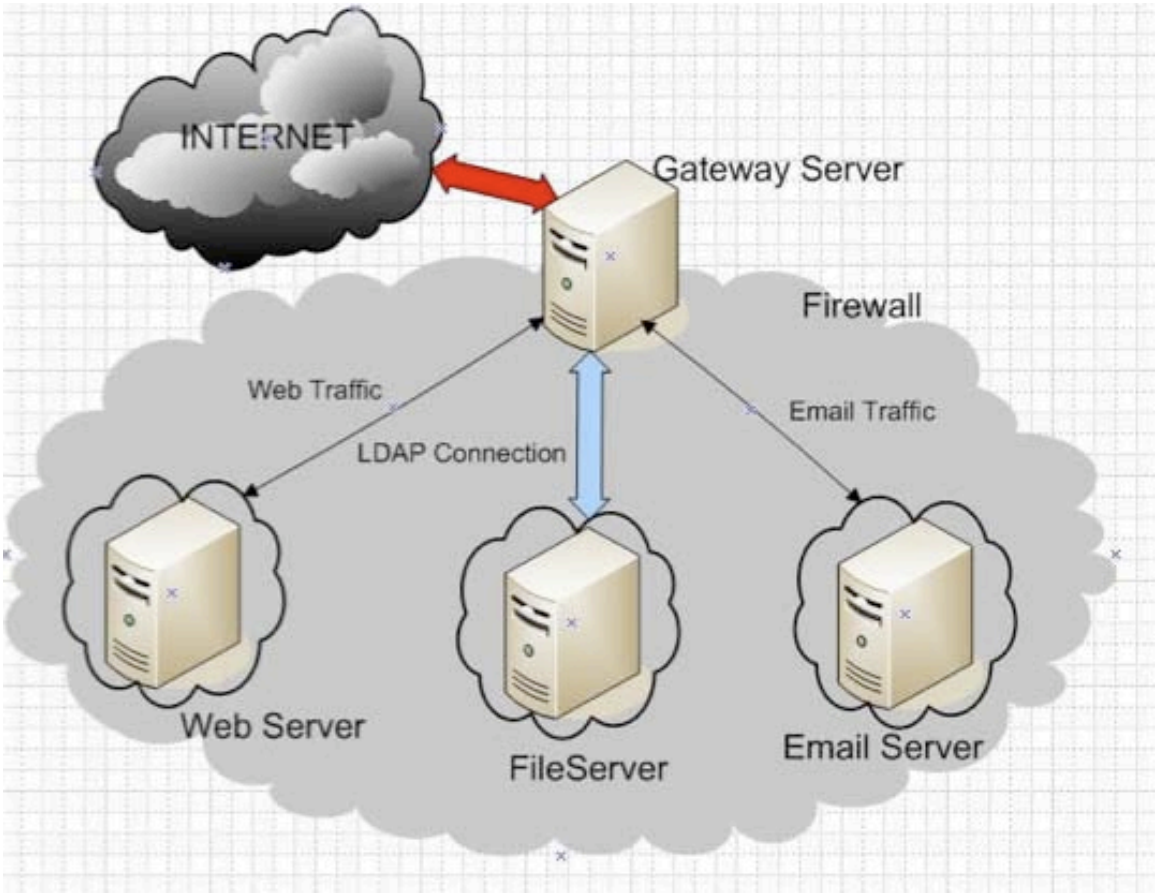
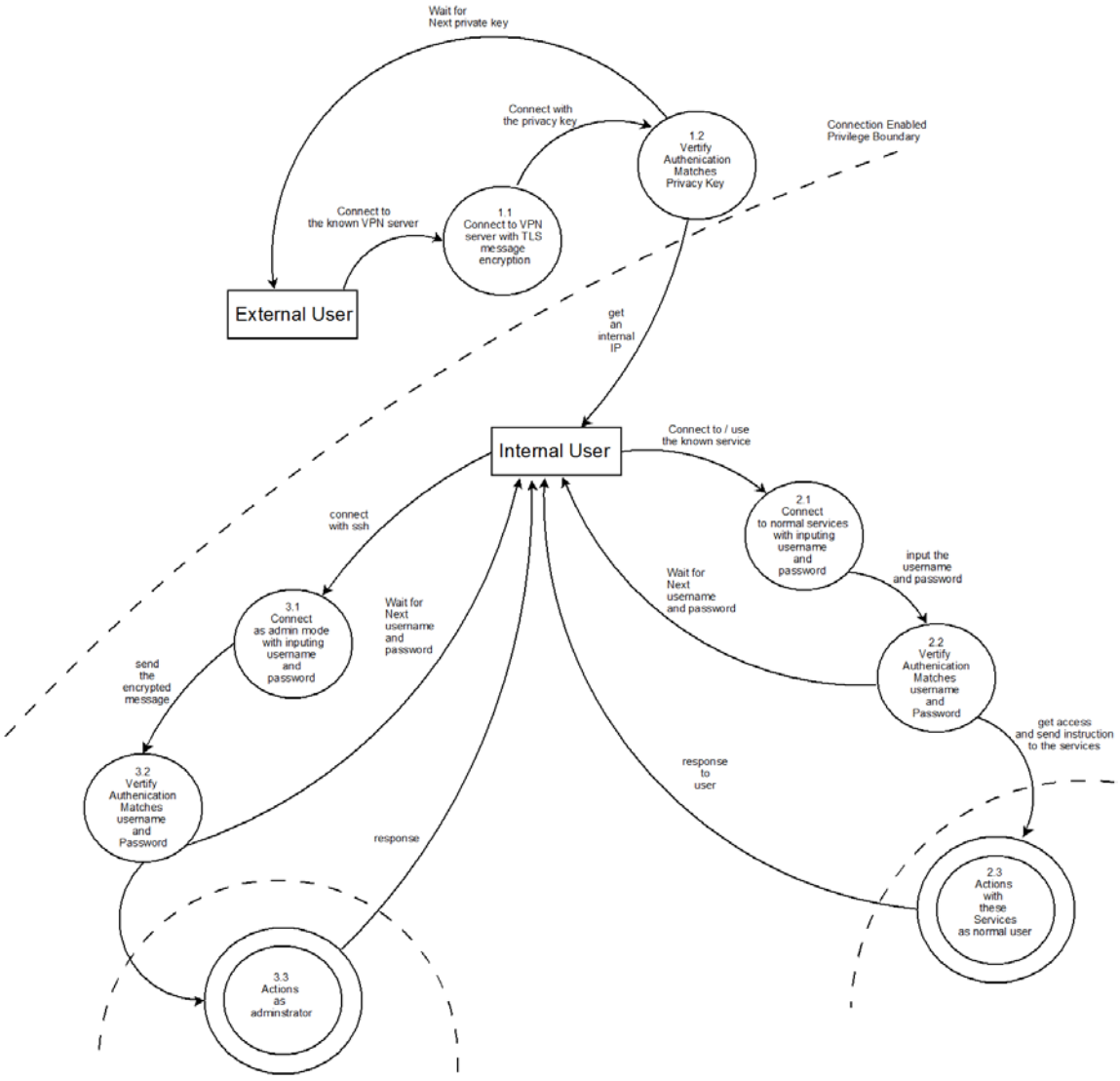


Figure A-2 Level 0 diagram



10 Threats

Threats and other information that the user should be aware of, to prevent possible vulnerabilities.

Threat – Access to the internal web page information

ID	1
Name	The adversary gains unauthorized access to the information on the internal web page.
Description	Internal web page is for internal employees of the company to share technical details of the projects, discussion forums, client information, upcoming project ideas etc. The information shared here will be internal to the company and should be viewable only by the current employees of the company
STRIDE Classification	• Information Disclosure
Mitigated?	NO
Known Mitigation	10 & 11
Entry Points	1, 2, & 3
Assets	3
Threat Tree	Refer to Threat Tree 1

Threat – Bandwidth Reduction (External) (DoS)

ID	2
Name	The adversary can send multiple packets to gateway machine, reducing or completely denying bandwidth between company network & internet.
Description	Adversary floods gateway with traffic, interfering or denying data flow in and out of internal company network. Business communications and project collaborations with clients are affected. While internal web is still running fine.
STRIDE Classification	• Denial of Service
Mitigated?	NO
Known Mitigation	10 & 11
Entry Points	1 & 2
Assets	0 & 4
Threat Tree	Refer to Threat Tree 2

Note for above: A possible solution for this can be blocking machines after a fixed number of failed login attempts. The router should prompt for a challenge response in order to remove it from the router's block list.

Threat – Unauthorized access to super computer

ID	**3**
Name	Adversary gains access to super computer & top secret project info.
Description	Adversary gains access to shared network resources by infiltrating company's internal network. Depending upon access level can spread and gain access to high-level company resources connected to virtual work environment.
STRIDE Classification	• Tampering • Repudiation • Information Disclosure
Mitigated?	NO
Known Mitigation	1, 2, & 3
Entry Points	1, 2, & 3
Assets	0, 1, 1.2, 2.1, & 3
Threat Tree	Refer to Threat Tree 3

Threat – Unauthorized access to an email account of another user

ID	4
Name	The adversary gains access to email account of another user
Description	An adversary creates his own account on the email server or gets access to accounts of other users.
STRIDE Classification	• Information Disclosure • Elevation of Privilege
Mitigated?	NO
Known Mitigation	1 & 2
Entry Points	1 & 1.1
Assets	2, 2.1, & 3
Threat Tree	Refer to Threat Tree 4

Threat – An insider gains access to file share of other users or other departments

ID	5
Name	An insider gains access to file share of other users or other departments.
Description	An insider is able to load the file share of other users which will give him unauthorized access to the files of other users and departments.
STRIDE Classification	• Tampering • Information Disclosure
Mitigated?	NO
Known Mitigation	1 & 2
Entry Points	1.1 & 4
Assets	2, 2.1, & 3
Threat Tree	Refer to Threat Tree 5

Threat – Internal / External users accessing ssh service on the servers

ID	6
Name	An Internal / External users accessing ssh service on the servers.
Description	An internal / external user tries to ssh into a server machine. If the user knows the ssh port (22), which is the standard port, he can try to guess the username such as admin, administrator etc and brute force the password.
STRIDE Classification	• Tampering • Elevation of Privilege
Mitigated?	NO
Known Mitigation	1 & 2
Entry Points	1.1 & 2
Assets	0, 1.2, 2, 2.1
Threat Tree	Refer to Threat Tree 6

11 Vulnerabilities

ID	**1**
Name	Access to internal web page information
Description	Hijack private IP and gain access to internal network, essentially spoofing.
STRIDE classification	Information disclosure
DREAD	(D1 = 5, R = 9, E = 10, A =10, D2 = 8) / 5 = 8.4
Cor. Threat	1

ID	**2**
Name	Bandwidth reduction (DDoS)
Description	Denial of service for internet connection caused by an adversary on the internet.
STRIDE classification	DoS
DREAD	(D1 = 10, R = 7, E = 9, A =10, D2 = 6) / 5 = 8.4
Cor. Threat	2

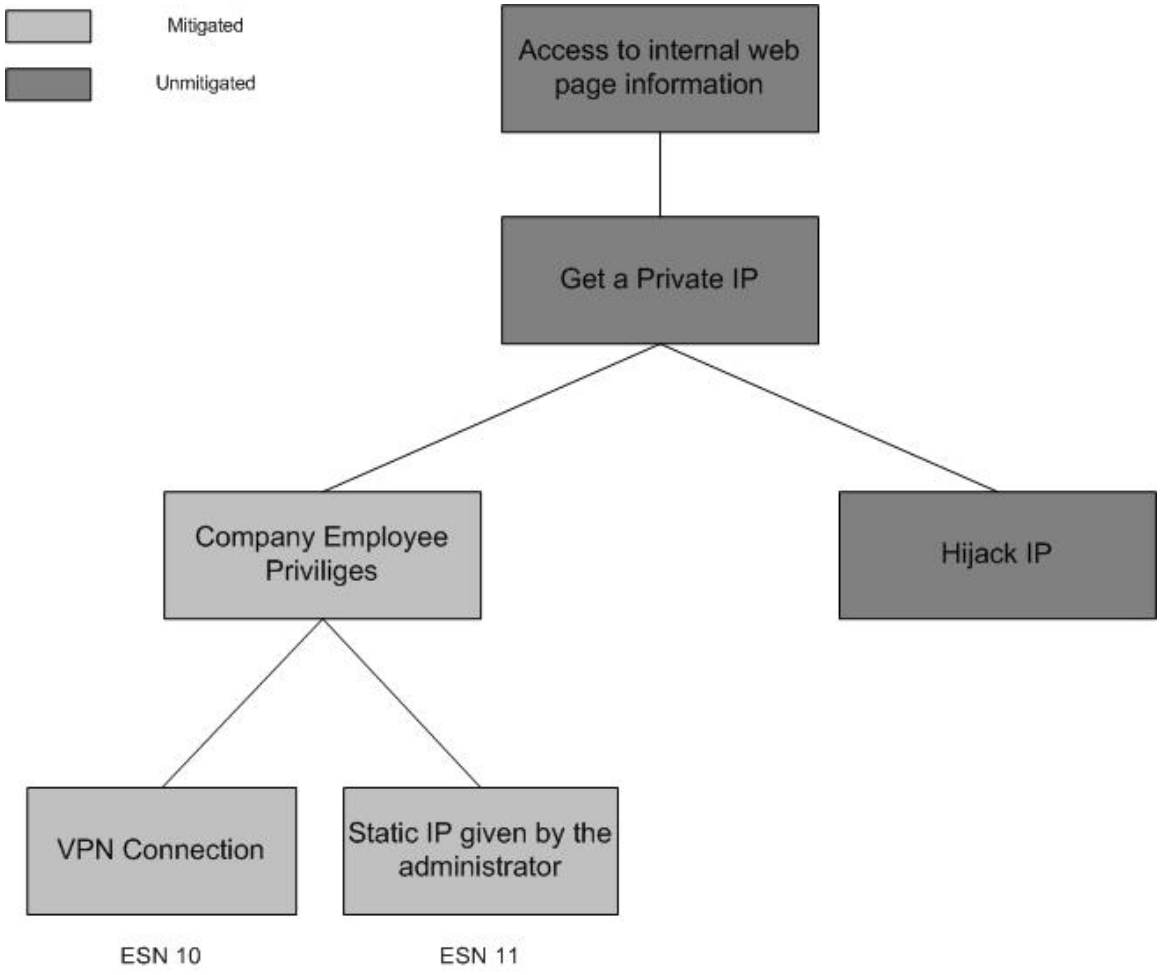
ID	**3**
Name	Adversary gains access to super computer & top secret project info.
Description	Adversary could guess passwords by brute force cracking, or gain physical access to cause damage.
STRIDE classification	Spoofing Tampering Repudiation Information Disclosure Elevation of Privilege
DREAD	(D1 = 9, R = 9, E = 10, A =10, D2 = 7) / 5 = 9
Cor. Threat	3

ID	**4**
Name	Access to e0mail account of another user
Description	Adversary can brute force crack passwords and gain uses' mail account access. From here they could acquire more sensitive information about accounts, projects, or user access.
STRIDE classification	Spoofing Tampering Repudiation Information Disclosure Elevation of Privilege
DREAD	(D1 = 6, R = 7, E = 10, A =7, D2 = 9) / 5 = 7.8
Cor. Threat	4

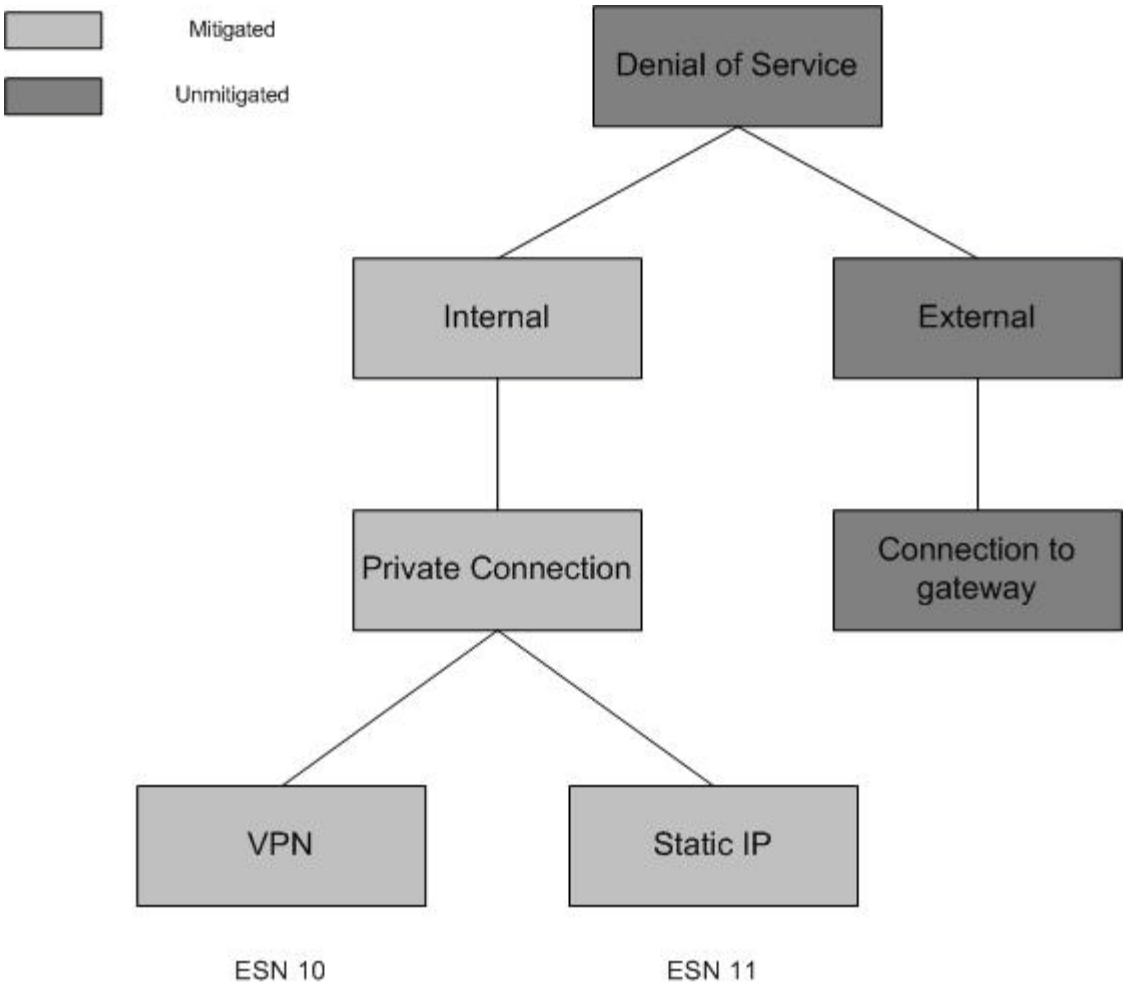
ID	**5**
Name	Access to other users & departments files
Description	Brute force cracking of user passwords allow adversary to gain access to user/admin accounts.
STRIDE classification	Spoofing Tampering Repudiation Information Disclosure Elevation of Privilege
DREAD	(D1 = 9, R = 8, E = 7, A =9, D2 = 6) / 5 = 7.8
Cor. Threat	5

ID	**6**
Name	ssh to server
Description	Brute force password cracking and unsecure user names could give adversary ssh access, once the ssh port is discovered through port scanning methods.
STRIDE classification	Spoofing Information Disclosure Elevation of Privilege
DREAD	(D1 = 10, R = 8, E = 10, A =6, D2 = 8) / 5 = 8.4
Cor. Threat	6

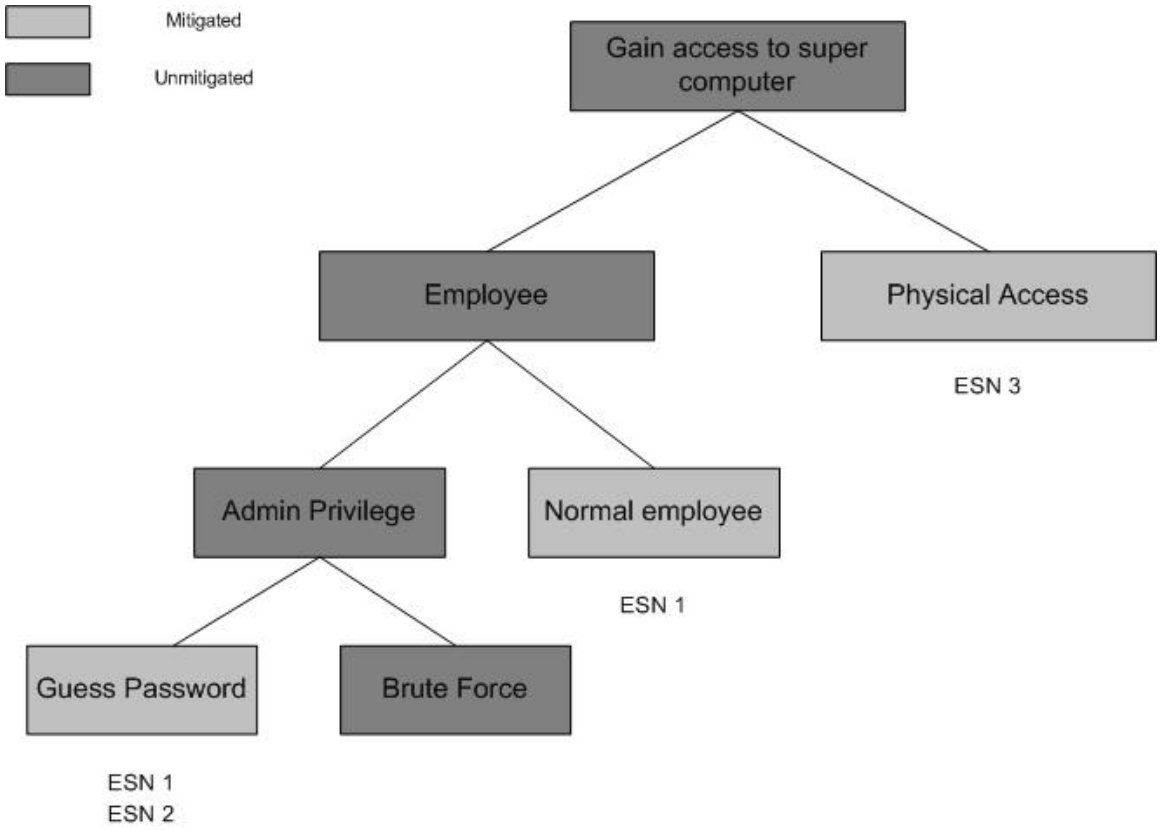
12 Threat Trees



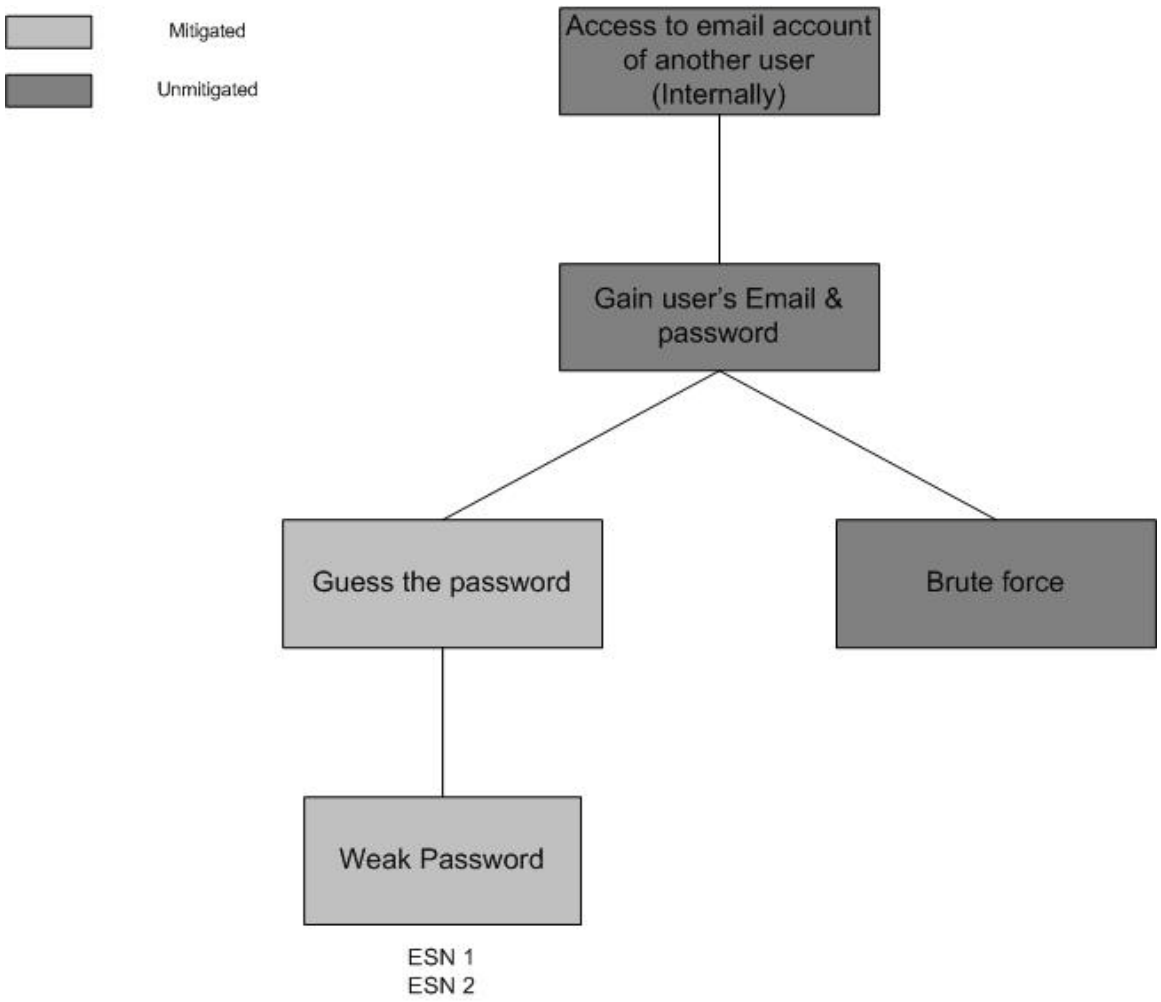
Threat Tree 1



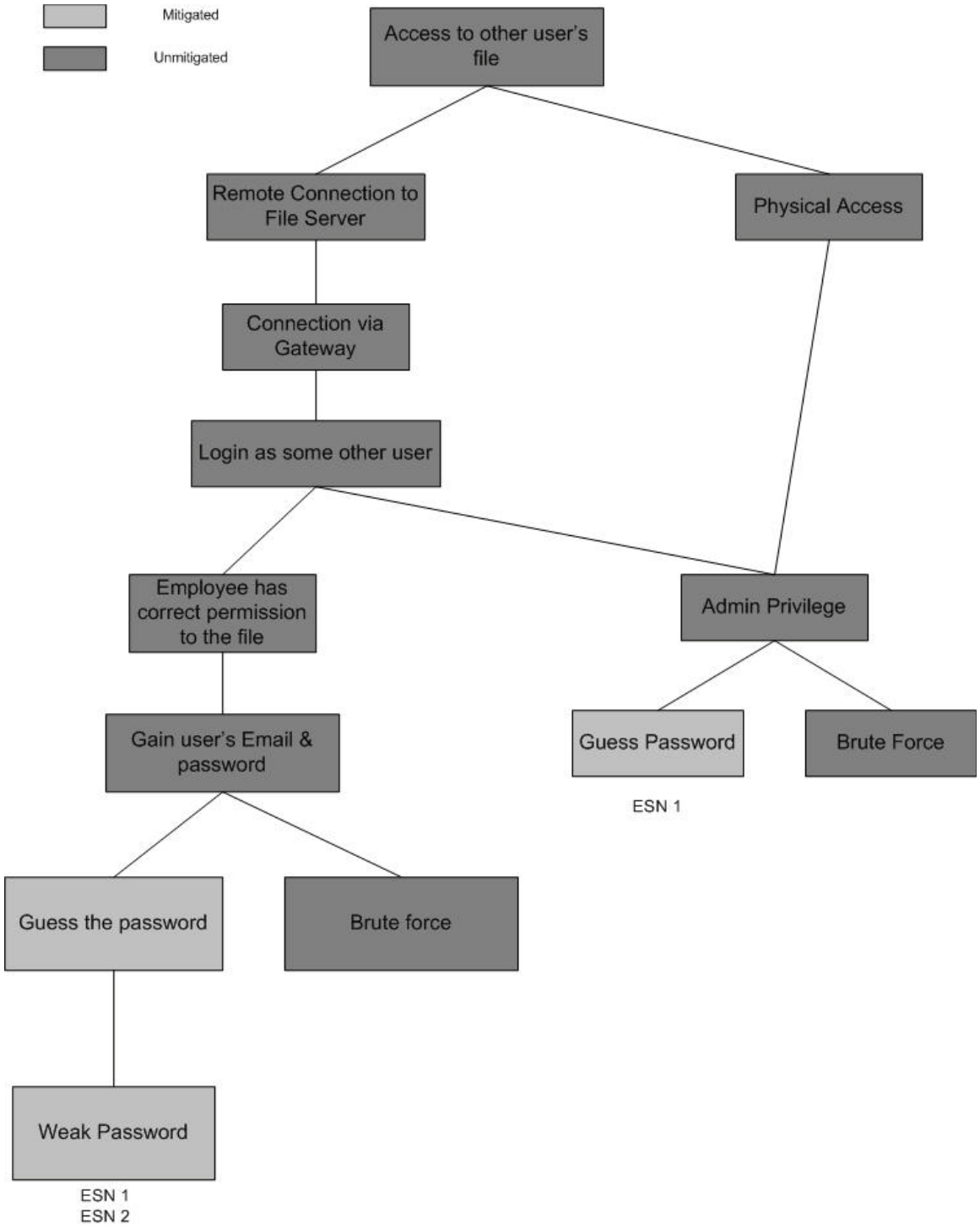
Threat Tree 2



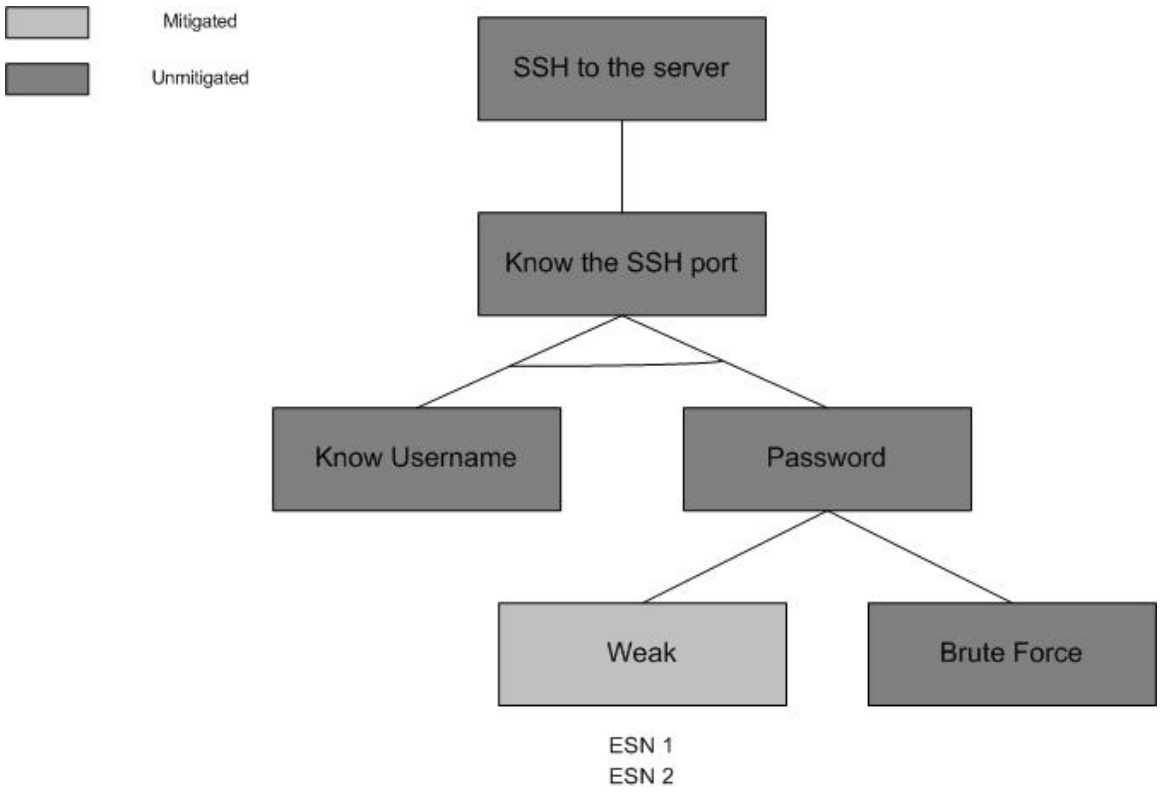
Threat Tree 3



Threat Tree 4



Threat Tree 5



Threat Tree 6

Summary

Administering complex systems such as ERIS' requires thorough attention to threats against the system architecture and the data within. Employing robust security measures are essential to maintaining important systems.

Through threat modeling our system architecture, we found that all of the threats identified are not mitigated. This can be attributed to a very basic installation of the servers and services with fairly simple security measures.

Given time and resources, the ERIS? Group will meet the ongoing challenges that face all systems administrators: hardening the security of servers, services, topologies, and client machines. The ERIS Group will continue to advance our system security development in order to maintain high-level data protection our customers expect.